Independent claim 1 recites:

> 1. A method for an authentication process within a distributed data processing system, the method comprising:
>
> receiving an attribute certificate from a client at a host within the distributed data processing system;
>
> extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;
>
> decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and
>
> forwarding the authentication data to a controlled resource.

The rejection of claims 1, 4, 12, 14, 17, 25, and 28 states in its entirety:

> As per claims 1, 4, 12, 14, 17, 25, and 28, Parker teaches receiving an attribute certificate within a distributed data processing system including authentication information, (Col 1 lines 40-45. Parker teaches forwarding the data to a controlled resource (applications, Col 1 lines 45-50).
>
> Parker does not teach encryption.
>
> Riggins teaches encryption of messages with the public key of the recipient, (Col 2, lines 15-25).
>
> It would have been obvious to one of ordinary skill in the art to include the encryption of Riggins with the certificate of Parker, because the encryption makes the communication secure.

Applicant acknowledges that Parker teaches a privilege attribute certificate (PAC) that contains user privilege attribute information. However, it is confusing why the rejection states that Parker does not teach encryption as it is clear that Parker does teach encryption; Parker teaches the use of encryption keys, though it does not teach the use of public key certificates in the manner of the present invention or in the manner of Riggins. Likewise, Applicant also acknowledges that Riggins teaches encryption of messages with public keys.

However, the rejection does not explain or even attempt to address the specific steps in the method of claim 1, etc.. In other words, the rejection completely fails to address each

element of claim 1, e.g., such as receipt of an attribute certificate, extracting encrypted authentication data from the received attribute certificate, decrypting the encrypted authentication data, and then using the decrypted authentication data with respect to the controlled resource. Hence, the rejection completely fails to present a proper obviousness analysis in the obviousness-type rejection.

Moreover, Parker and/or Riggins, either as individual references or as a hypothetical system that combines the teachings of the two references, fail to disclose the claimed elements of the claims, particular the elements of independent claim that were summarized in the paragraph immediately above and completely copied in a paragraph hereinabove. In particular, Parker teaches an older type of privilege attribute certificate that does not simply convey attribute information within a digital certificate but also includes an encryption key within the attribute certificate. Thus, the attribute certificate carries not only a set of attributes for a user/client but also an encryption key from a user/client. However, claim 1 specifically recites that the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host, not the client; the encrypted authentication data is then decrypted by the host with a private key associated with the host. Thus, the system of Parker in which a user/client sends along an encryption key within an attribute certificate to a host employs a completely different encryption mechanism than is employed with the present invention, which uses an encryption system of public key/private key pairs.

More importantly, one of ordinary skill in the art would not have been motivated to combine the teachings of Parker and Riggins because of the different encryption mechanisms that are

employed within the systems that are disclosed in these two references. Although Riggins discloses the use of an encryption

system that employs public key/private key pairs, a hypothetical system that combines the teachings of Parker and with teachings from another reference would not require the encryption mechanism of Riggins because the system of Parker discloses that an encryption key is carried within an attribute certificate from a user/client to a host. In other words, since the host receives an encryption key from the user/client, there would be no motivation for one of ordinary skill in the art to look to Riggins because the encryption mechanisms are different; it would be illogical for one having ordinary skill in the art to combine different encryption mechanisms in the manner that the rejection simply asserts that one having ordinary skill in the art would have done. In this manner, Riggins can be said to teach away from Parker.

Moreover, a hypothetical system that combines the teachings of Riggins into the system that is disclosed by Parker would obviate the need for the encryption key that is included in the attribute certificate of Parker because the host in Riggins already has access to a different encryption key. Hence, the rejection's proposed modification renders Parker unsuitable for its intended purpose. As stated in MPEP 2143.01:

> If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

In addition, in the present invention, the attribute certificate carries authentication information for the user/client to the host for subsequent access to controlled resources, such as legacy applications that the user/client is attempting to use and that require an authentication procedure that can be satisfied by the authentication information (which Applicant reiterates is not disclosed in the applied prior art

references). In a hypothetical system as asserted in the rejection, it would be illogical for the attribute certificate to

carry an encryption key that has been used to encrypt the authentication data that is also carried in the attribute certificate because the authentication data would not be secure. Thus, the hypothetical system that is proposed by the rejection would not be secure, which is contrary to the motivational statement that is provided by the rejection.

Independent claim 1 is directed to a method; independent claim 12 is directed to a data structure; independent claim 14 is directed to an apparatus; and independent claim 25 is directed to a computer program product. The Office action uses an obviousness argument against claims 12, 14, and 25 and their dependent claims by relying on the arguments that are used against claim 1 and its dependent claims. Applicant's arguments with respect to the rejection of claim 1 are similarly applicable against the rejection of claims 12, 14, and 25 and their dependent claims.

Examiner bears the burden of establishing a *prima facie* case of obviousness

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Only when a *prima facie* case of obviousness is established does the burden shift to the applicant to produce evidence of nonobviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Rijckaert*, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). If the Patent Office does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). In response to

an assertion of obviousness by the Patent Office, the applicant

may attack the Patent Office's *prima facie* determination as improperly made out, present objective evidence tending to support a conclusion of nonobviousness, or both. *In re Fritch*, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780, 1783 (Fed. Cir. 1992).

Parker and Riggins clearly fail to disclose at least one feature of the present invention as recited within each independent claim, notwithstanding the arguments presented by the Office action, thereby rendering Parker and Riggins incapable of being used as primary and secondary references as argued by the current rejection. Moreover, a hypothetical combination of Parker and Riggins would also fail to reach the claimed invention of the present patent application. As should be recognized, because both the primary and secondary references in the rejection fail to disclose the claimed features against which the references were applied, and because the references fail to be combinable to produce these claimed features, the rejection fails to fulfill the requirements of a proper obviousness argument.

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

IV. 35 U.S.C. § 103(a)—Obviousness

The Office action has rejected claims 2, 3, 5, 6, 9, 11, 13, 15, 16, 18, 19, 22, 24, 26, 27, 29, 30, 33, and 35 under 35 U.S.C. § 103(a) as unpatentable over Parker in view of Riggins and further in view of Olden or Butt. These rejections are traversed.

The remaining claims recite various claim elements, such as using the method of claim 1 with respect to legacy applications or wherein the attribute certificate has an X.509 certificate format. As argued above, the hypothetical combination of Parker and Riggins fails to reach the claimed invention of the present patent application as recited in independent claims 1, 12, 14, and 25. As should be recognized, because both the primary and secondary references in the rejection fail to disclose the features against which the references were applied, and because the references fail to be combinable to produce these claimed features, the rejection fails to fulfill the requirements of a proper obviousness argument with respect to dependent claims 2, 3, 5, 6, 9, 11, 13, 15, 16, 18, 19, 22, 24, 26, 27, 29, 30, 33, and 35 that depend from independent claims 1, 12, 14, and 25.

V. 35 U.S.C. § 103(a)—Obviousness—*Riggins* in view of *Multerer*

The Office action has rejected claims 8, 10, 21, 23, 32, and 34 under 35 U.S.C. § 103(a) as unpatentable over Riggins in view of Multerer et al., "Multi-server Location-Independent Authentication Certificate Management System", U.S. Patent Number 6,134,658, filed 06/09/1997, issued 10/17/2000. This rejection is traversed.

Independent claim 10 reads:

> 10. A method for obtaining a digital certificate, the method comprising:
>
> retrieving a public key certificate associated with a host within a distributed data processing system;

extracting a public key associated with the host from the public key certificate;

encrypting with the public key authentication data for a controlled resource at the host;

generating a request for an attribute certificate;

storing the encrypted authentication data within the request for the attribute certificate;

sending the request for the attribute certificate to an attribute-certificate-issuing authority; and

receiving an attribute certificate from the attribute-certificate-issuing authority, wherein the attribute certificate comprises the encrypted authentication data.

The rejection of claims 8, 10, 21, 23, 32, and 34 reads in its entirety:

> As per claim 10, Riggins teaches exchange of public key certificates. Riggins teaches acquiring a public key from said certificate and using it for encrypting further communications (Col 2 lines 11-23).
>
> Riggins does not disclose an attribute certificate exchange.
>
> Multerer teaches generating a request for a certificate (Col 6 lines 62-66). Multerer teaches storing authentication data within the request (Col 6 lines 56-59). Multerer teaches sending the request to a certificate authority (Col 7 lines 3-6). Multerer teaches receiving a certificate from the certificate authority wherein the certificate comprises the encrypted authentication data (Col 7 lines 7-17).
>
> It would have been obvious to one of ordinary skill in the art to combine the encryption of Riggins with the certificate exchange of Multerer because the encryption increases the security of the transaction.

Applicant acknowledges that Riggins teaches the use of public key/private key pairs. Applicant also acknowledges that Multerer et al. teaches the features of generating a request for a certificate, storing authentication data within the request, sending the request to a certificate authority, and receiving a certificate from the certificate authority. However, the rejection states that the system of Multerer et al. generates a certificate "wherein the certificate comprises the encrypted authentication data (Col 7 lines 7-17)". This is clearly incorrect. Multerer et al. states at column 7, lines 7-17:

> The authentication certificate granting authority CA1 receives the transmitted data at step 304, reviews the received data, verifies the identity of the requester. If the received data matches the requester validating information that is available to the authentication certificate granting authority CA1, the authentication certificate authority CA1 generated the signed authentication certificate. At step 305, the authentication certificate granting authority CA1 transmits the issued authentication certificate 502 back to the requesting party, server S1, in encrypted form for installation on the requester's processor.

Thus, the authentication certificate granting authority CA1 in the system of Multerer et al., which the rejection is implicitly suggesting is equivalent to the attribute-certificate-issuing authority in the present invention, is merely encrypting the entire certificate for transmittal back to the requestor. Multerer et al. does not disclose the encryption of the authentication data in the manner of the present invention, i.e., as stated in claim 10, wherein the authentication data has been encrypted with the public key of the host. First, in the system of Multerer et al., the authentication certificate granting authority CA1 encrypts the entire certificate for return to the requester. Second, the authentication certificate granting authority CA1 would encrypt the entire certificate with the public key of the requester, which would decrypt the entire certificate with its private key, thereby securing the transmittal of the certificate as a whole between the authentication certificate granting authority CA1 and the requester.

Applicant also notes that because of the use of "the" to qualify "the encrypted authentication data" and the rules of claim construction, Applicant is not referring to just any type of encryption but is referring to the resulting data of the

specific steps that are recited in the claim to specifically encrypt the authentication data.

In addition, Applicant agrees with the rejection that Riggins fails to disclose an attribute certificate exchange or, more relevant to the subject matter in claim 10, the generation of an attribute certificate. Applicant would expect that the rejection would then explain the manner in which Multerer et al. discloses the use of an attribute certificate. However, the rejection fails to do so, and more importantly, Multerer et al. also completely fails to disclose the usage of an attribute certificate or the generation of an attribute certificate.

Moreover, the rejection completely fails to address most of the elements of claim 10. The present invention is not merely putting authentication data into a digital certificate, as presented by the rejection, and the present invention is not merely employing digital certificates and their associated public key/private key pairs to encrypt data or to digitally sign data. Claim 10 recites a specific sequence of multiple steps in which particular data is encrypted with particular encryption keys for a particular purpose. The rejection completely ignores the significance of the claimed sequence of steps.

More importantly, FIG. 5 of Multerer et al. clearly shows that the digital certificate 502 that is generated by the authentication certificate granting authority CA1 is a novel type of public key certificate; it contains a copy of the user/client's public key. In contrast, the present invention is generating and using a novel type of attribute certificate. The detailed specification of the present application clearly acknowledges the prior art existence of attribute certificates, and it was known in the prior art that an attribute certificate is a type of digital certificate that is distinct from a public key certificate. An attribute certificate often accompanies or is accompanied by a public key certificate within a transaction

in which a user/client is attempting to access a controlled resource at a host. However, an attribute certificate does not

contain a copy of the public key of the user/client; if it did, then a transaction would not require the use of a public key certificate, or more specifically, the reasons and advantages for separating information into attribute certificates and public key certificates would cease to be necessary.

Thus, Applicant asserts that a hypothetical system that combines the teachings of Multerer et al. into the system that is disclosed by Riggins would obviate the need for any attribute certificate because the system would already all necessary data within its version of a public key certificate. Hence, the rejection's proposed modification renders Multerer et al. unsuitable for its intended purpose. As stated in MPEP 2143.01:

> If the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification.

In conclusion, Riggins and Multerer et al. clearly fail to disclose at least one feature of the present invention as recited within each independent claim, notwithstanding the arguments presented by the Office action, thereby rendering Riggins and Multerer et al. incapable of being used as primary and secondary references as argued by the current rejection. Moreover, a hypothetical combination of Riggins and Multerer et al. would also fail to reach the claimed invention of the present patent application. As should be recognized, because both the primary and secondary references in the rejection fail to disclose the claimed features against which the references were applied, and because the references fail to be combinable to produce these claimed features, the rejection fails to fulfill the requirements of a proper obviousness argument.

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used

the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited

prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

VI. Conclusion

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: October 10, 2006

Respectfully submitted,

Jeffrey S. LaBaw
Reg. No. 31,633
ATTORNEY FOR APPLICANT